Application No. 09/468,230
Docket No. 87355.1100

PATENT
Customer No. 30734

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES
APPEAL BRIEF FOR THE APPELLANTS

Ex parte Liebl

Applicant: Troy J. LIEBL)
)
Serial No. 09/468,230) Group Art Unit: 2131
)
Filed: December 21, 1999) Examiner: Christian A. LAFORGIA

For: DIAGNOSTIC TOOL SECURITY KEY

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are three (3) copies of a corrected Appeal Brief in response to the Notification of Non-compliant Appeal Brief mailed March 24, 2005. The corrected Brief is due by April 25, 2005 (April 24, 2005 is a Sunday). Please charge any fee deficiencies or credit any overpayments to Deposit Account No. 50-2036.

Respectfully submitted,

BAKER & HOSTETLER LLP

P. Alan Larson

P. Alan Larson
Registration No. 53,184

Date: 4/25/05

Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 861-1500
Fax: (202) 861-1783

Application No. 09/468,230
Docket No. 87355.1100

PATENT
Customer No. 30734

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES
APPEAL BRIEF FOR THE APPELLANTS
Ex parte Berdan, *et al.*

Applicant: Troy J. LIEBL	)	
	)	
Serial No. 09/468,230	)	Group Art Unit: 2131
	)	
Filed: December 21, 1999	)	Examiner: Christian A. LAFORGIA

For: DIAGNOSTIC TOOL SECURITY KEY

BRIEF ON APPEAL

I. INTRODUCTION

This is an appeal from the final Office Action dated March 30, 2004. A Notice of Appeal was filed on August 30, 2004.

II. REAL PARTY IN INTEREST

The Real Party in Interest in the present application is SPX Corporation by way of an assignment.

III. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to the appellant, appellant's representatives or assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

IV. STATUS OF THE CLAIMS

Claims 1-29 are pending in the application. Claims 1-7, 11-17 and 21-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Sasaki*, U.S. Patent No. 6,134,488, (hereinafter, "*Sasaki*"). Claims 8-10 and 18-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Sasaki* in view of U.S. Patent No. 6,148,400 to *Arnold* (hereinafter, "*Arnold*"). Claims on appeal, claims 1-29, are set forth in the attached Appendix 1.

V. STATUS OF THE AMENDMENTS

An Amendment submitted after the Final Office Action on June 30, 2004, was not entered.

VI. SUMMARY OF THE INVENTION

A. Related Art Problems Overcome by the Invention

In the conventional art, passwords have been widely utilized to prevent unauthorized access to stand-alone computer systems. Most computer networks utilize passwords to prevent unauthorized access to network resources. Some of these passwords are encrypted to prevent sniffers from determining the passwords when they are transmitted over unsecure transmission paths. In addition, various electronic media have included passwords to prevent illegitimate possessors of the electronic media from utilizing software on the method. While passwords may prevent an illegitimate possessor of the electronic media from utilizing software stored on the media, a password alone will not prevent a legitimate purchaser from utilizing software stored on the media in an unauthorized manner.

In order to alleviate the problems of the prior art, the invention of the present application provides a system for preventing the unauthorized downloading or software into a diagnostic tool.

The embodiments of the present invention of the present application provide a technique for hampering unauthorized utilization of software with multiple diagnostic tools.

B. The Claimed Invention

1. Independent Claim 1

The method of independent claim 1 and its dependant claims is described in the specification, *inter alia*, at pg. 11, lines 3-23 through pg. 12, lines 1-17 and FIGS. 1 and 4B.

Independent claim 1 includes a method for preventing unauthorized downloading of software into a diagnostic tool 100, comprising the steps of providing a first external storage device 132 that is electrically coupled to the diagnostic tool 100, the first external storage device 132 including a first security signature, providing a second external storage device 130 that is electrically coupled to the diagnostic tool 100, the second external storage device 130 including software, and downloading 412 the software into an internal storage device 116 of the diagnostic tool when a second security signature included within the diagnostic tool 100 is the same as the first security signature included within the first external storage device 132.

2. Dependent Claims 2-10

Dependent claim 2 is dependent on claim 1 and further defines the method wherein the first external storage device 132 is a smart card that provides the first security signature to the diagnostic tool 100 through a smart card reader.

Dependent claim 3 is dependent on claim 1and further defines the method wherein the second external storage device 130 is electrically coupled to the diagnostic tool 100 through a serial port 106.

Dependent claim 4 is dependent on claim 3 and further defines the method wherein the serial port 106 is a USB port.

Dependent claim 5 is dependent on claim 3 and further defines the method wherein the serial port 106 is a RS232 port.

Dependent claim 6 is dependent on claim 3 and further defines the method wherein the serial port 106 is an IrDA compatible infrared port.

Dependent claim 7 is dependent on claim 3 and further defines the method wherein the serial port 106 is an IEEE 1394 port.

Dependent claim 8 is dependent on claim 1 and further comprises the step of modifying 418 the first security signature upon successful downloading of the software into the internal storage device 116 located within the diagnostic tool 100.

Dependent claim 9 is dependent on claim 8 and further defines the method wherein the first security signature is modified 418 so that it cannot be further utilized to download the software into any diagnostic tool 100.

Dependent claim 10 is dependent on claim 9 and further defines the method wherein the first security signature is erased 418.

3. Independent Claim 11

The apparatus of independent claim 11 and its dependant claims is described in the specification, *inter alia,* at pg. 5, lines 16-23 through pg. 6, lines 1-22 and FIG. 1.

Independent claim 11 is a diagnostic tool 100 for communicating with a plurality of motor vehicle control units, the diagnostic tool 100 preventing the unauthorized downloading of software into the diagnostic tool 100, the diagnostic tool 100 comprising a processor 102 for controlling the downloading of software into the diagnostic tool 100, a first port 128 for electrically coupling the processor 102 to a first storage device 132, the first storage device 132 including a first security signature, and a second port 106 for electrically coupling the processor 102 to a second storage device 130, the second storage device 130 including software, wherein the diagnostic tool 100 downloads the software into a third storage device 116 located within the diagnostic tool 100 when a second security signature stored within the diagnostic tool 100 is the same as the first security signature included within the first storage device 132.

4. <u>Dependent Claims 12-23</u>

Dependent claim 12 is dependent on and is the diagnostic tool 100 of claim 11, and further defines the method wherein the first storage device 132 is a smart card that provides the first security signature to the diagnostic tool 100 through a smart card reader.

Dependent claim 13 is dependent on and is the diagnostic tool 100 of claim 11, and further defines the method wherein the second storage device 130 is electrically coupled to the diagnostic tool 100 through a serial port 106.

Dependent claim 14 is dependent on and is the diagnostic tool 100 of claim 13, and further defines wherein the serial port 106 is a USB port.

Dependent claim 15 is dependent on and is a diagnostic tool 100 of claim 13, and further defines wherein the serial port 106 is a RS232 port.

Dependent claim 16 is dependent on and is the diagnostic tool 100 of claim 13, and further defines wherein the serial port 106 is an IrDA compatible infrared port.

Dependent claim 17 is dependent on and is the diagnostic tool 100 of claim 13, and further defines wherein the serial port 106 is an IEEE 1394 port.

Dependent claim 18 is dependent on and is the diagnostic tool 100 of claim 11, and further defines wherein the processor 102 causes the first security signature to be modified upon successful downloading of the software into the third storage device 116 located within the diagnostic tool 100.

Dependent claim 19 is dependent on and is the diagnostic tool 100 of claim 18, and further defines wherein the first security signature is modified so that it cannot be further utilized to download the software into any diagnostic tool 100.

Dependent claim 20 is dependent on and is the diagnostic tool 100 of claim 19, and further defines wherein the first security signature is erased.

Dependent claim 21 is dependent on and is the diagnostic tool 100 of claim 11, and further defines wherein the first storage device 132 is a smart card and the second storage device 130 is a flash ROM.

Dependent claim 22 is dependent on and is the diagnostic tool 100 of claim 11, and further defines wherein the first storage device 132 is a smart card and the second storage device 130 is an EEPROM.

Dependent claim 23 is dependent on and is the diagnostic tool 100 of claim 11, and further defines the method including a keypad 112 coupled to the processor 102 for receiving input from a user, the user initiating the downloading of the software by selecting a particular menu item from a list of menu items, and a display 104 coupled to the processor 102 for providing the list of menu items to the user of the diagnostic tool 100.

5. Independent Claim 24

The method of independent claim 24 and its dependant claims is described in the specification, *inter alia*, at pg. 11, lines 3-23 through pg. 12, lines 1-17 and FIGS. 1 and 4A.

Independent claim 24 includes a method for preventing unauthorized downloading of software into a diagnostic tool 100, comprising the steps of providing an external storage device 130 that is electrically coupled to the diagnostic tool 100, the external storage device 130 including a first security signature and software, and downloading 427 the software into a memory 114 of the diagnostic tool 100 when a second security signature included within the diagnostic tool 100 is the same as the first security signature included within the external storage device 130.

6. Dependent Claims 25-26

Dependent claim 25 is dependent on claim 24 and further defines the method including the step of storing 428 the second security signature of the diagnostic tool 100 as the first security signature on the external storage device 130 when the first security signature is determined to be a default value.

Dependent claim 26 is dependent on claim 24 and further defines the method wherein the external storage device 130 is a flash ROM.

7. Independent Claim 27

The apparatus of independent claim 27 and its dependant claims is described in the specification, *inter alia,* at pg. 5, lines 16-23 through pg. 6, lines 1-22 and FIG. 1.

Independent claim 27 is a diagnostic tool 100 for communicating with a plurality of motor vehicle control units, the diagnostic tool 100 preventing the unauthorized downloading of software by the diagnostic tool 100, the diagnostic tool 100 comprising a processor 102 for executing the software, a port 106 for electrically coupling the processor 102 to an external storage device 130, the external storage device 130 including a first security signature and software, where the diagnostic tool 100 downloads the software into a memory 114 of the diagnostic tool 100 when a second security signature included within the diagnostic tool 100 is the same as the first security signature included within the external storage device 130.

8. Dependent Claims 28 and 29

Dependent claim 28 is dependent on claim 27, and further defines the method wherein the processor 102 causes the second security signature of the diagnostic tool 100 to be stored as the first security signature on the external storage device 130 when the first security signature is determined to be a default value.

Dependent claim 29 is dependent on claim 27 and further defines the method wherein the external storage device 130 is a flash ROM.

VII. ISSUES

A. Whether claims 1-7, 11-17 and 21-29 are patentable under 35 U.S.C. §103(a) over *Sasaki* (U.S. Patent No. 6,134,488).

B. Whether claims 8-10 and 18-20 are patentable under 35 U.S.C. §103 (a) over *Sasaki* in view of *Arnold* (U.S. Patent No. 6,148,400).

VIII. GROUPING OF CLAIMS

Each claim of this patent application is separately patentable, and upon issuance of a patent, will be entitled to a separate presumption of validity under 35 U.S.C. §282.

IX. APPELLANTS ARGUMENTS

The Applicant respectfully submits that none of the prior art, specifically *Sasaki, et al.* and *Arnold,* either separately or in combination, teach or suggest the method or apparatus recited in the pending claims. For example, the Examiner rejected claims 1-7, 11-17 and 21-29 under 35 U.S.C. § 103(a) as being unpatentable over *Sasaki, et al.* The Applicant respectfully disagrees with the Examiner's conclusion.

To establish a prima facie case at obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves, or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the Applicant's disclosure. See M.P.E.P. § 2142; In re Vaeck, 947 F.2d 488 (Fed. Cir. 1991).

At least, two of these three basic criteria are not met. There is no suggestion or motivation to combine references to arrive at the claim in mention, and, the prior art reference does not teach or suggest all of the claimed limitations. For example, *Sasaki* does not teach or suggest the method recited in claim 1, including a "first external storage device including a first security signature" and "downloading the software into an internal storage device of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the first external storage device." The Examiner, in addressing the insufficiency of *Sasaki* to teach or suggest the invention of claim 1 and its dependent claims, merely states in a conclusory fashion, on page 4 of the final Office Action, that "It would have been obvious to one of ordinary skill in the art at the time the invention was made to include two security signatures." However, a statement that modifications of the prior art to meet the claimed invention would have been well within the ordinary skill of the art at the time the claim of the invention was made, is not sufficient by itself to establish prima facie obviousness. See, for example, M.P.E.P. § 2143.01. See, also, *Al-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308 (Fed. Cir. 1999). Without some objective reason to combine teachings of references, the prima facie case of obviousness is not met by the Examiner.

The Examiner also remarks, on page 4 of the Final Office Action, that "One would be motivated to include the signatures as it would create a method to ensure the external storage device was what it claimed to be." Here, the Examiner seems to state that the invention, itself, provides motivation to arrive at the invention. However, this is not the correct standard for providing motivation, the prior art must provide motivation, not the disclosure of the present invention. See M.P.E.P. § 2142.

The Examiner, on page 4 of the final Office Action, remarks that instances of using an external storage device with matching signature authentication can be seen in U.S. Patent No. 5,525,672, hereinafter, "*Chainer, et al.*" However, the Examiner makes no argument that *Chainer, et al.* cures the insufficiencies of *Sasaki* and, indeed, *Chainer, et al.* and *Sasaki*, either separately, or in combination, do not teach or suggest the method recited by independent claim 1 and its dependent claims. *Sasaki* and *Chainer* are discussed below.

Sasaki is directed to a diagnostic tool that forces an activation signal to a target portion of a vehicle being diagnosed. The diagnostic tool detects the current state of the target portion and compares the current state with a state predicted when the activation signal is sent to the target portion. A signal to stop a self diagnosis test for the target portion, which can vary due to the activation signal, is also sent to the vehicle. The diagnostic tool includes a ROM card 7 that contains: (1) a diagnostic item management table 71 for use to select diagnostic items unique to engine type according to the ECU code; (2) a vehicle diagnostic program storage area 72 for storing a vehicle diagnostic program related to a plurality of diagnostic items; (3) a standard data storage area 73 for storing standard data commonly used for a plurality types of the vehicles irrespective of the type of the ECU mounted thereon; and (4) a unique data storage area 74 for storing unique data, the contents of which may vary according to each individual ECU. (Col. 5, lines 8-19). ROM 7 can store new or changed information, such as when a new car is introduced. ROM 7 can also store the vehicle diagnostic system and the information contained therein can be read into the CPU through the ROM card interface. (Col. 4, lines 50-58).

Sasaki does not teach that the information from the ROM is downloaded into a storage device in the diagnostic tool. After diagnosis is completed, the operator then causes the vehicle diagnostic apparatus 2 to transmit the data on the diagnostic results of several vehicles from the transmitter 24 to a host machine, such as a host computer 30, which includes a mass storage device 33. (Col. 4, line 65 – Col. 5, line 3). In the host computer 30, a plurality of data sets, each representing the diagnostic results transferred in the plural data sets, are then incorporated into one unit and stored into the storage device 33. (Col. 15, lines 23-37). The transmission shown in Fig. 1 is unidirectional and no software is indicated as being transferred to the vehicle diagnostic apparatus 2 from the host computer. Thus, software can not be downloaded from a second storage device into the diagnostic tool or that the second storage device can transmit any security signature for that matter.

Chainer is directed to an event recorder that attaches to a machine or vehicle, which can broadcast an encrypted signature, thereby leaving behind an electronic version of a "fingerprint" of the machine or vehicle carrying the recorder. The fingerprint, captured by an external data acquisition system, provides a history of events related to the machine or vehicle. The event recorder includes a microcomputer, a memory, and a transceiver that are preferably housed in a tamper resistant casing. The memory stored signature information about the vehicle, such as the owner's name, license plate, vehicle registration, etc. In a first mode of operation, monitoring stations can periodically send an interrogation signal, such as when a radar gun detects that the vehicle is speeding. Upon receiving the interrogation signal, a smart card transmits the vehicle's signature information to the monitoring station where the time and date is stamped along with the speed of the vehicle.

In a second mode of operation, when a sensor detects a sudden or violent acceleration or deceleration, such as during a collision, an event recorder mounted in each car will begin transmitting its signature information and receiving and storing the other vehicle's signature information. It is important that the smart card from, which signature data was received, can be authenticated to ensure that the signature data has not been altered. The smart cards can be authenticated, yet duplication resistant, by employing zero-knowledge protocols. Zero knowledge protocols allow a smart card 101 to be authenticated and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart card is authentic without the smart card revealing its authentication information. (Col. 3, lines 28-56). The actual security signature information is not exchanged or required to be the same in order for something to happen, such as allowing a software to download into a tool.

As shown above, the references alone or in combination do not disclose all the elements claimed invention, such as a method for preventing unauthorized downloading of software that includes providing a first external storage device that is electrically coupled to the diagnostic tool, the first external storage device including a first security signature, providing a second external storage device that is electrically coupled to the diagnostic tool, the second external storage device including software, and downloading the software into an internal storage device of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the first external storage device, as recited in claim 1.

With respect to claim 11 and its dependent claims, 12-23, the references alone or combination also do not teach or suggest a diagnostic tool that includes a "first storage device including a first security signature," and a "second storage device including software, wherein the diagnostic tool downloads the software into a third storage device located within the diagnostic tool when a second security signature stored within the diagnostic tool is the same as the first security signature included within the first storage device," as recited in claim 11.

The second external device of *Sasaki* (host computer 30 and data storage 33) can not transmit any software or a security signature to the diagnostic tool because the transmission of information as shown in FIG. 1 is from the diagnostic tool to the host computer and not vice versa. Additionally, the second external device does not contain a second security signature. There is no downloading of the software into the diagnostic tool when a second security signature is the same as the first security signature because the references use zero knowledge authentication protocols, which do not share authentication information. Additionally, no software download into a storage device in the diagnostic tool is taught by the references.

With respect to claim 24 and its dependent claims, 25-26, the references, *Sasaki, et al.* and *Chainer, et al.,* alone or in combination, do not teach or suggest a method for preventing unauthorized downloading of software that includes "downloading the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device," as recited in claim 24.

With respect to independent claim 27 and its dependent claims 28-29, the cited references alone or combination do not teach or suggest a diagnostic tool that includes the "external storage device including a first security signature and software, where the diagnostic tool downloads the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device," as recited in claim 27. As stated above, the references do not disclose downloading software into a memory in the scan tool or that the download occurs when a first and second security signature are the same.

Further, there is no motivation to modify the references to arrive at the claimed invention. In fact, the prior art must suggest the desirability of the claimed invention. See, for example, M.P.E.P. § 2143.01. Here, the Examiner has shown no suggestion to modify the invention or a suggestion of the desirability of the claimed invention other than to say "one would be motivated to include the signatures as it would create a method to ensure the external storage device was what it claimed to be" on pages 4, 7 and 9 of the Final Office Action. Here, it appears that the Examiner is relying on the disclosure of the claimed invention, itself, to provide the motivation to arrive at the claimed invention, which clearly is not the standard for establishing prima facie obviousness. For a prima facie case of obviousness, it must be the prior art, not the invention that provides the motivation. See M.P.E.P. § 2142. Because the Examiner has failed to make a prima facie showing of obviousness, the Applicant respectfully requests the Board withdraw the Examiner's rejections of the claims under 35 U.S.C. § 103(a) in view of *Sasaki, et al.*

B. Whether or not claims 1-7, 11-17 and 21-29 are patentable for the reasons above, claims 8-10 and 18-20 are patentable at least for the reasons above and for the reasons described below.

Claims 8 and 18 include modifying the first security signature upon successful downloading of the software onto the internal storage device located within the diagnostic tool, while claims 9 and 19 further include the first security signature is modified so that it can not be further utilized to download the software into any diagnostic tool. *Arnold* (U.S. Patent No. 6,148,400) as stated by the Examiner deletes the private signature key after use. This of course, is not modifying the key because the key no longer exist, if it's deleted. Thus, *Sasaki* when combined with *Arnold* do not teach or suggest modifying the first signature after use.

Because claims 2-10; 12-23; 25, 26; and 28, 29 depend directly or indirectly from independent claims 1, 11, 24 and 27, respectively, that are believed to be in condition for allowance, these claims are also believed to be in condition for allowance.

X. CONCLUSION

For all of the above-noted reasons, it is strongly contended that certain, clear and important distinctions exist between the present invention as recited in claims 1-29 and the cited references as provided in the Office Action. It is further contended that these distinctions are more than sufficient to render the claimed invention unobvious to a person of ordinary skill in the art at the time the invention was made.

This final rejection being in error, therefore, it is respectfully requested that this Honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case, and indicate the allowability of claims 1-29.

In the event that this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. Please charge any fee deficiencies or credit any overpayments to Deposit Account No. 50-2036.

Respectfully submitted,

BAKER & HOSTETLER LLP

P. Alan Larson

P. Alan Larson
Registration No. 53,184

Date: 4/25/05

Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 861-1500
Fax: (202) 861-1783

APPENDIX 1

1. A method for preventing unauthorized downloading of software into a diagnostic tool, comprising the steps of:

providing a first external storage device that is electrically coupled to the diagnostic tool, the first external storage device including a first security signature;

providing a second external storage device that is electrically coupled to the diagnostic tool, the second external storage device including software; and

downloading the software into an internal storage device of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the first external storage device.

2. The method of claim 1, wherein the first external storage device is a smart card that provides the first security signature to the diagnostic tool through a smart card reader.

3. The method of claim 1, wherein the second external storage device is electrically coupled to the diagnostic tool through a serial port.

4. The method of claim 3, wherein the serial port is a USB port.

5. The method of claim 3, wherein the serial port is a RS232 port.

6. The method of claim 3, wherein the serial port is an IrDA compatible infrared port.

7. The method of claim 3, wherein the serial port is an IEEE 1394 port.

8. The method of claim 1, further comprising the step of:

modifying the first security signature upon successful downloading of the software into the internal storage device located within the diagnostic tool.

9. The method of claim 8, wherein the first security signature is modified so that it cannot be further utilized to download the software into any diagnostic tool.

10. The method of claim 9, wherein the first security signature is erased.

11. A diagnostic tool for communicating with a plurality of motor vehicle control units, the diagnostic tool preventing the unauthorized downloading of software into the diagnostic tool, the diagnostic tool comprising:

a processor for controlling the downloading of software into the diagnostic tool;

a first port for electrically coupling the processor to a first storage device, the first storage device including a first security signature; and

a second port for electrically coupling the processor to a second storage device, the second storage device including software, wherein the diagnostic tool downloads the software into a third storage device located within the diagnostic tool when a second security signature stored within the diagnostic tool is the same as the first security signature included within the first storage device.

12. The diagnostic tool of claim 11, wherein the first storage device is a smart card that provides the first security signature to the diagnostic tool through a smart card reader.

13. The diagnostic tool of claim 11, wherein the second storage device is electrically coupled to the diagnostic tool through a serial port.

14. The diagnostic tool of claim 13, wherein the serial port is a USB port.

15. The diagnostic tool of claim 13, wherein the serial port is a RS232 port.

16. The diagnostic tool of claim 13, wherein the serial port is an IrDA compatible infrared port.

17. The diagnostic tool of claim 13, wherein the serial port is an IEEE 1394 port.

18. The diagnostic tool of claim 11, wherein the processor causes the first security signature to be modified upon successful downloading of the software into the third storage device located within the diagnostic tool.

19. The diagnostic tool of claim 18, wherein the first security signature is modified so that it cannot be further utilized to download the software into any diagnostic tool.

20. The diagnostic tool of claim 19, wherein the first security signature is erased.

21. The diagnostic tool of claim 11, wherein the first storage device is a smart card and the second storage device is a flash ROM.

22. The diagnostic tool of claim 11, wherein the first storage device is a smart card and the second storage device is an EEPROM.

23. The diagnostic tool of claim 11, further including:

a keypad coupled to the processor for receiving input from a user, the user initiating the downloading of the software by selecting a particular menu item from a list of menu items; and

a display coupled to the processor for providing the list of menu items to the user of the diagnostic tool.

24. A method for preventing unauthorized downloading of software into a diagnostic tool, comprising the steps of:

providing an external storage device that is electrically coupled to the diagnostic tool, the external storage device including a first security signature and software; and

downloading the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device.

25. The method of claim 24, further including the step of :

storing the second security signature of the diagnostic tool as the first security signature on the external storage device when the first security signature is determined to be a default value.

26. The method of claim 24, wherein the external storage device is a flash ROM.

27. A diagnostic tool for communicating with a plurality of motor vehicle control units, the diagnostic tool preventing the unauthorized downloading of software by the diagnostic tool, the diagnostic tool comprising:

a processor for executing the software;

a port for electrically coupling the processor to an external storage device, the external storage device including a first security signature and software, where the diagnostic tool downloads the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device.

28. The diagnostic tool of claim 27, wherein the processor causes the second security signature of the diagnostic tool to be stored as the first security signature on the external storage device when the first security signature is determined to be a default value.

29. The diagnostic tool of claim 27, wherein the external storage device is a flash ROM.